Social and Legal Implications of Digital Identity in a Multi-national Environment

Sergio Sánchez
DIATEL – Universidad Politécnica de Madrid
sergio@diatel.upm.es

Emilia Pérez
DIATEL – Universidad Politécnica de Madrid
belleboni@diatel.upm.es

Ana Gómez
DIATEL – Universidad Politécnica de Madrid
agomez@diatel.upm.es

Justo Carracedo
DIATEL – Universidad Politécnica de Madrid
carracedo@diatel.upm.es

Abstract

The i2010 e-Government Action Plan from the European Union forces Public Administrations (national, regional and local) of all Member States that by 2010 to meet all administrative acts of the citizens through the Internet. This implies the need for mechanisms and systems to be able to unequivocally identify people on the Internet, together with a reliable system of interoperable electronic identification management (eIDM), in such a way that citizens, businesses and government departments (even in different Member States) can identify themselves and certify their transactions accurately, quickly and simply.

However, despite the clear advantages that this entails for EU citizens, namely the fact that they possess a digital identity which allows them secure and identified access to the services offered by the various public administrations in Member States, the implementation of a solution of this kind involves a series of risks which, if they are not duly dealt with, may engender a reduction in the effectiveness of public institutions and citizens' trust in them. This article will analyse the problems associated with digital identity in the EU framework and the extent to which the solutions adopted to date meet the constitutional requirements, or fail to, highlighting aspects which may entail a risk or detriment to the freedoms of citizens and those relating to the handling of digital identity which have not yet been tackled but which, given their particular relevance, necessitate an immediate solution.

1. Introduction

In 2006, the European Union launched its i2010 e-Government Action Plan [1], aiming to modernize the public services of Member States and to make them more effective, offering secure services to reduce the administrative burden and inefficiency with which citizens today are faced. Within this concept of modernization and improvement, a fundamental requirement is that of cross-border continuity of public services, so that transactions involving public administrations of different states may be carried out.

As an immediate consequence of the application of this Plan, we find that governments (at local, regional and national level) of all member states are obliged to handle all citizens' administrative needs via the Internet, by a rapidly approaching deadline. This involves implementing a series of additional measures, both at national and international level which, through their direct impact on citizens, highlight the need for people to have a digital identity which allows them to prove their identity unequivocally when carrying out operations online.

In this article we will use the definitions of identity and digital identity of an entity, found in [2], understanding that a citizen is an entity that must be identified within a communications infrastructure. The afore-mentioned document states that an entity, and therefore a citizen, has one unique identity which consists of a determined set of attributes that do not necessarily need to be unique to said entity, but which are useful in that, as a whole, they enable this entity to be distinguished from another. A digital identity is, by definition, a subset (or partial identity) of the identity of an entity expressed in electronic format and may be considered as the entity's representation on the net. In accordance with this definition, a given entity will have multiple digital identities, which may be unique or otherwise.

In order to identify their citizens, some European countries have traditionally used systems based on showing a document issued by the State proving their identity (national ID card). This document has evolved over time, from a simple sheet of paper with a set of personal information, certified by an official authority, to the most recent identity documents. The content of these is virtually similar in all countries, and they are equipped with strong anti-counterfeit measures such as a photograph, signature and fingerprint, which allow for biometric, and presumably, more reliable identification of the owner.

Both in countries which already have traditional identification systems and in those which don't, citizens will need an electronic or digital identity which allows them to identify themselves on the net, with at least the same guarantees as those who do so with their national ID card in inter-personal interactions. To this end, the majority of countries in the European Union are rolling out infrastructure which will allow all citizens to be sent electronic identification cards known as eID cards, within

a reasonable period of time. Their external appearance will be very similar to that of traditional identification documents, but with the safeguard that they include a chip storing information on the citizen's identity. These eID cards are already being sent out in Austria, Belgium, Estonia, Finland, Italy, Portugal, Sweden and Spain. However, in other countries like Sweden or Denmark having an ID card is not compulsory, they use electronic identities that are only valid in the net.

The i2010 Plan does not currently consider that traditional identity cards must evolve towards eID cards, as the first cards designed to be used in public services were related to the security of the State, for example, to facilitate border control, whereas electronic identification seeks to facilitate access to public services as well as to provide personalised services. However, countries such as Spain have opted to combine the functions of both types of card in one single document, so that the current identity cards (13 million copies of which have already been sent out at the end of 2009,) combine citizens' personal and biometric data together with their digital identity (secret and certified private key).

Notwithstanding the advantages that possessing a digital identity undoubtedly entails for EU citizens, allowing them secure and identified access to services provided by the different public administrations of member states, the implementation of this solution is not free from risks which, if they are not duly tackled, could impair the effectiveness of State institutions and the trust of citizens therein.

This article will analyse the problems associated with digital identity in the EU framework, and will consider the extent to which the solutions adopted to date meet the constitutional requirements, highlighting aspects which may entail a risk or detriment to the freedoms of citizens and those relating to the treatment of digital identity which have not yet been tackled but which, given their particular relevance, require an immediate solution.

2. Problems associated with digital identity in the EU framework

This section will identify the risks which may arise when rolling out the electronic identity system, together with the main problems which must be solved in order to achieve effective pan-European communication between all levels of government.

This article will not discuss the risks inherent to any process of registration and authentication, given the fact that malicious elements may make undue use of a citizen's credentials (and thus obtain their electronic identity), or they may take over their electronic identity and therefore, from the point of view of the internet, take on their real identity. Any of these circumstances may cause significant harm, including the loss of integrity and confidentiality of information and the loss of availability and function of a service, thereby entailing risks of financial loss for institutions and citizens and even risks to their personal safety.

Due to the significance of this problem, great effort has been made for some years now to ensure that the process of registering citizens with the Registry Authorities is imbued with maximum guarantees of security, forcing these Authorities to carry out exhaustive checks on the credentials presented and obliging them to maintain strict internal security measures. Likewise, Certification Authorities, which are also equipped with strong internal security measures, are required to maintain a constantly-updated record of the state of citizens' identities (valid, revoked and expired), as well as providing mechanisms so that citizens can easily revoke a digital identity that they believe to have been compromised.

As such, perhaps the aspect needing to be strengthened concerns citizens, as they must be aware of the risks involved in possessing a digital identity and the need to protect it at all times. A detailed study of the risks involved in the registration and authentication processes, their potential impact on institutions and citizens and the probabilities of occurrence can be found in [3].

2.1. The problem of identity management based on certificates

Another important challenge which digital identification systems must tackle is cross-border continuity of public services; namely, that a citizen not come up against barriers which are difficult, or even impossible to cross, in order to access public services offered by different countries. For example, today a Spanish citizen can work for a German company and carry out their professional activity in Belgium, theoretically without any kind of red tape. However, in this multi-national environment, when the worker wishes to access the services offered by the German Public Administration with their national ID card issued in Spain, or to consult information on work-related aspects within the Belgian Public Administration, problems arise due to the need to prove the citizen's identity by means of a certificate issued by an entity in a different country to where the service is being requested.

Nowadays certificates are usually based on the X.509 standard and they contain almost the same data. However there are many problems, for example, there is not a top level Certification Authority that would enable revocation checks or certificate path validation. The existence of this Authority, would undoubtedly help to resolve many of the current problems, but poses enormous political and legal difficulties for its management, hence currently solutions are oriented towards achieving interoperability among existing identity systems at a pan-European level.

Generically, owing to the diversity of identity management systems, when the user of a given system – whether a citizen, an enterprise or the government itself – seeks to communicate with governments outside the scope of his or her own local identity management system, management systems must be linked to each other and understand each other so that the identity of the user of one system can be understood and accepted by the other system.

It is therefore necessary to establish an interoperability framework at the European Union level for identity management systems. It should include the specification and development of a set of technical and organizational infrastructures that could define, administer and manage attributes related to the identity of individuals. These infrastructures are called Identity Management Systems or IDMs and it is expected that their use at European Union level will be available in a short period of time due to the restrictions and simplifications derived from the environment where they are going to be applied, the Public Administration. In this environment is feasible to consider that involved entities are trustworthy, so they will not act badly or fraudulently.

In order to successfully establish the interoperability framework, European Union has drawn up a roadmap [4]. In this roadmap, a series of design principles will be laid out, based around the fundamental principle of subsidiarity, namely, each Member State must maintain its autonomy and responsibility to continue its Identity Management Systems initiatives. These principles give rise to a series of criteria for a pan-European Identity Management System:

- Federated. There must be mutual trust between the different governments regarding the methods of identification and authentication.
- Multi-level. In the sense that it must allow Member states to provide multiple levels of security for identity management services. The requirements for authentication for each service must be adapted to the security need of said service, which involves the pan-European definition of a set of criteria for each level of authentication.
- Depending on reliable sources. To guarantee the quality of information, in each Member state there must be one single reliable source for each piece of information corresponding to a registered entity, so that data duplication is avoided and one single correct and official source is ensured.
- Allow the private sector to be incorporated in member states where private companies are trusted, for example financial institutions, in order to provide electronic identity management services.

We can therefore deduce from this that identity federation refers to a shared effort to achieve the interoperability of Identity Management Systems that are present in different environments. In this way information on a user's identity, possibly spread across different areas, may be brought together so that the user can be identified in one environment and can have access to others. As such, the different service providers can access the user's information in the different environments.

The identity federation extends the use of a user's digital identity, so that it goes from being something internal for a service provider, to being shared with several providers. This change prompts the appearance of complicated management processes related to the way in which identity is registered, revoked and modified within an identity provider, thereby engendering greater security risks for the Identity Federation [5].

On the basis of action plans launched by the European Union, in recent years a number of initiatives have focused on achieving pan-European interoperability between identity management systems [6][7][8][9]. Basically, all these initiatives culminate in the proposed creation of security infrastructure based on a federated model. These models rely on a series of identity portals in each Member State responsible for authenticating entities at a national level and deciding the trust level granted to authentication processes in another Member State, so that each State will accept as equivalents the authentication levels and mechanisms used in another State on the basis of a set of criteria, while no specific pan-European infrastructure would be required. In this way it can separate provision of the service from processes related to digital identity that are necessary to provide said service – i.e., user registration, generation and storage of identity and authentication data.

With respect to outstanding problems that require a solution, that of trust is perhaps the most important. The heterogeneity of existing systems and the mechanisms of authentication and authorization operating in different countries makes it crucial to equip a pan-European system with the capacity to map identity tokens delivered by the identity management system of one country to its counterparts in another country, if the objective is to make access to services as transparent as possible to the public and users in general. This means that the system must necessarily be multi-level. The fact that the system is multi-level also facilitates, a priori, the incorporation of all countries with digital identity and an identity management system, thus speeding up the implementation of the system.

Another issue to be solved is semantic interoperability, which is closely linked to multilevel operability. Incorporation within a pan-European system of solutions that have already been implemented at a national level demands translation between representation formats at interconnection points, which also implies a need to establish a certain degree of semantic interoperability.

Despite the existence of the roadmap, the design principles and the afore-mentioned criteria, we can confirm that in practice, interoperability between identity management systems in various European countries continues to be an ambition rather than reality, although solutions are being proposed.

2.2. Problems of electronic signatures

In addition to the problems of interoperability between different identity management systems discussed above, there are other interoperability problems that have a greater impact and therefore must be considered, specifically speaking, and the problem of interoperability of electronic signatures. This problem arises because current European legislation allows for anybody possessing an eID to use it to sign any piece of information going to a recipient who may be located in a different EU country. This means that the entity receiving a signed document must be able to verify the signature, irrespective of the eID used by the signing entity.

The interoperability challenges are thus best described from the viewpoint of the receiver of a digitally signed piece of information, because it must check all signatures, handling the relevant signature formats including all necessary modes (enveloped, enveloping, and independent) for multiple signatures, all necessary hash and crypto algorithms and the eIDs of all signers.

Although the technical validation of signatures has its challenges with respect to scaling, the real problem to receiver party is the assessment of the risk implied by accepting the signature, determined by the legal situation, the quality of the cryptography used, the liability situation, and the trustworthiness of the Certification Authority. With the objective of solving these problems, the European project PEPPOL [10] is developing guidelines, specifications and pilot solutions to overcome the lack of interoperability between national schemes for electronically signing tender documents, which gives rise to the hope that these problems will disappear and the process of signature verification can be carried out with full guarantees.

2.3. Protection of personal data

Throughout a large part of history, identity has been understood from the legal point of view, as solely a tool to validate the subject of the rights, obligations and punishments or penalties should they fail to comply with the law. Only with constitutional recognition of individual freedoms enshrined in the first constitutions, did identity also become an expression of individual freedom. In fact, it wasn't until the beginning of the 19th century that identity as an aspect of personality began to be recognised by legislation as something capable of adequately expressing the individual personality and people's freedoms.

Currently, a natural person's identity is not systematically regulated by legislation. There are a set of definitions which do not always concur and which have two fundamental functions: i) Allowing identification for legal ends; ii) Protecting individual rights and freedoms related to a natural person. As regards regulation, it may be said that personal identity is regulated at different levels, as it is dealt with in national constitutions, in the European Union treaty, in private legislations of each nation, in administrative legislation and is furthermore protected against non-authorised use and access by third parties, through criminal law.

Generically speaking, we can say that a method of identification which allows an individual to be distinguished from all others, must, from a legal perspective, comply with two fundamental rules:

- Show sufficient information to guarantee the highest level of security possible when it comes to differentiating between one individual and others.
- Not reveal information which corresponds to the private level of the individual to be identified.

Normally, and to comply with this, each legal system avails of a store of information within their identification documents, which usually corresponds to a biometric image of one or several parts of the body of the subject to be identified. This is true for Spanish identity cards. In some countries such as Austria or the United Kingdom, it is not compulsory to carry any kind of identification document, unlike in other countries such as Spain, Italy or Germany, where this is compulsory.

On the other hand, specific information such as civil status or profession, typically held by Public Administrations, is considered to be superfluous in current legislation on personal identification, basically because it is too closely linked to the individual's private sphere. The current public interest in ever-more specific identification must give way before the individual's rights and freedoms. In the more democratic legal systems, legislation has made clear moves towards identification systems which, while being less precise, are also less intrusive than traditional systems. The principle that official identification should show no information relating to the private life of the subject to be identified can currently be considered as a widely accepted rule.

With the aim of building citizens' trust in electronic identification systems and of unifying legislation, the European Directive 95/46/CE was established, on data protection [11]. The target of this is to grant the subject as great a control as possible over their identity and personal data, putting forward a series of requirements to be met by recipients, controllers, processors and third parties when processing this information. In this context,

personal data is understood to mean "any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

Thus, among the principles established by this Directive, the following should be highlighted:

- Personal data must be adequately processed and must fully comply with provisions in the law, it must be recognised with explicit and legitimate ends, be relevant and adequate to these ends (never excessive) and be used in accordance with them. This principle extends to cooperation between governments which is needed to collect specific data from a specific citizen, which will entail that a government request this data from another government, on behalf of or representing this citizen.
- Data identifying an individual should not be retained longer than necessary and individuals must be provided with means of control, to rectify, delete or block access to their personal data, furthermore adopting appropriate measures, from both technical and organisational perspectives, to prevent non-authorised access to or illegitimate use of data.
- Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for said data.

However, despite the existence of these principles which are applicable to personal data, there is much reluctance towards the possibility of including additional information on the holder in electronic identification cards, thereby giving the State greater control over the citizen (for example including information on their political ideology, religious beliefs, socially rejected diseases or allowing their movements to be traced). This fear is even greater when, such as in Spain's case, one single document includes all information required for authentication, both in services relating to security of the state and in those relating to interaction between the citizen and the Government. Therefore, one of the challenges to those facing digital identification systems is that of giving them maximum transparency, so that citizens harbour no suspicions on the nature of the personal data borne by the card that they carry.

2.4. Identity Delegation

The problem of identifying citizens in a pan-European environment is not the only one. There are other problems related to the different legal frameworks and different ways identity is used in each country. Of these problems, the most significant and most relevant one, owing both to its complexity and the fact that it is in demand from the public, is identity delegation. Present law in many Member States of the EU allows for delegation to another party in dealings with public institutions. For example, in Spain, one person can authorize another person, commonly a specialized management agency, to perform all transactions related to filing tax returns with the government. Thus, a person can have different roles simultaneously in an identity management system: one can be both an individual and the legal representative of an enterprise or organization. The identity management systems proposed to date have made very little progress in these issues and none provides support for role management and delegation.

The concept of identity delegation is defined [2] as the process in which an identified entity issues a mandate to another identified entity. On the basis of this definition, we can see that the act of delegating is a cession by a person or entity of part of its rights to another in order to enable the latter to act on behalf of the former before a third party. In terms of citizens and public institutions, delegation basically involves one citizen granting another citizen authorization or a mandate that the latter can use, in the name of the former, to access services provided by institutions.

According to [12] at least three parties are involved in the process of delegation: the delegator, the delegatee and the service provider. The delegator is a person or entity that shares, by means of what is usually called a delegation assertion, one or more of its privileges in accessing a service with another person or entity. The delegatee is the person who receives the privileges of the delegator, that is, the delegation assertion, and the service provider is the party which, as its own name indicates, provides certain services on demand to the delegatee after the delegation assertion has been presented. In addition to these generic entities, and depending on the delegation process used, other entities may emerge, such as the identity provider or delegation authorities.

Taking this set of basic entities as a point of departure, [13] presents a classification of delegation in two elementary models: the model of direct delegation and the model of indirect delegation. Direct delegation is when the delegator delegates all or a subset of his or her privileges to the delegatee, who makes use of them to access a service (Fig. 1). The same process applies in indirect delegation, but through a series of intermediate delegatees, as shown in Fig. 2.

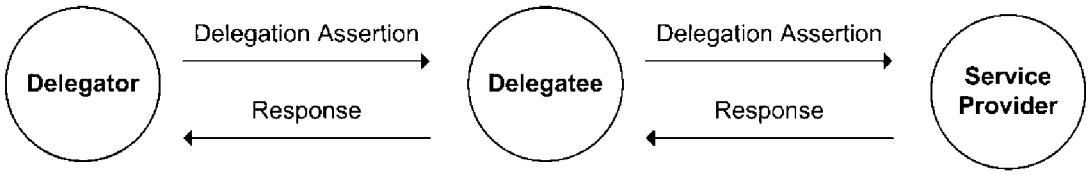

Figure 1 – Model of direct delegation

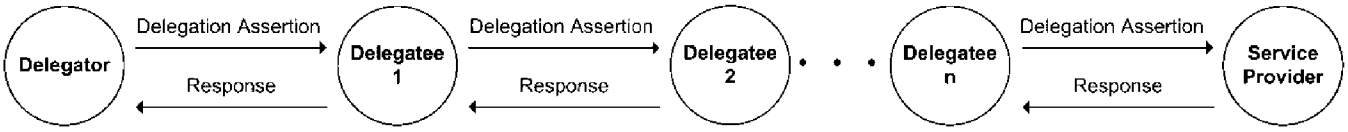

Figure 2 – Model of indirect delegation

We would highlight a series of aspects of delegation that were mentioned in [13]. The first is that delegation does not mean authorization. That is, even if a service provider accepts the delegation, it need not accept the privileges requested by the delegatee. It is always at the discretion of the service provider whether or not to accept the request made by the delegatee. Secondly, the delegation assertion must always prove consent on the part of the delegator, as the latter may impose certain conditions on the act of delegation such as a period of validity or permission to engage in indirect delegation. Finally, any solution must always seek to preserve the privacy of the delegator.

To date, and despite being one of the aspects that citizens request when accessing services, identity management systems which are being rolled out across different EU member countries do not contemplate the possibility of delegation, basically due to the technical and legal difficulties involved. No technical solution has been proposed which would enable a shared and interoperable identity delegation model facilitating delegation mechanisms which a citizen from a specific country could use, for example granting a representative of another country access to and interaction with determined public services. As such, there is no specific legislation at European level regulating delegation in such important aspects as who may delegate, who they may delegate to, for which services delegation may occur or how many levels of delegation are allowed in case the use of indirect delegation is enabled.

3. Conclusions

Movement of citizens of member countries within the European Union for work or for study are becoming increasingly commonplace, and everything would seem to indicate that this trend will increase as cooperation between countries in the EU extends and the number of European-wide projects and initiatives grows. On the other hand, it is foreseeable that the number of people who travel within Europe for personal reasons will also rise, for example, the case of retired people who change their place of residence because they would prefer to live in peaceful areas but who wish to keep their nationality of origin.

Due to the increasing movement of citizens, and with the aim of meeting the new needs of these people, the exchange of information between governments of different European countries will also expand. As such, the forms and mechanisms used by citizens to deal with their local, regional, national and supranational governments will vary, so that the operations can be carried out remotely.

The gradual but definite distribution of electronic identities promoted by Public Administrations provides essential elements for the implementation of electronic Identity Management systems (eIDMs) which will permit this type of interaction, but there are still technical, social and legal problems arising from the use of these systems and their interoperability. The level of acceptance of identification systems is far from equal in all European Union member states and the legislation and standards are not uniform, thereby prompting significant doubts among citizens as to the convenience or otherwise, of the use of this type of system. This matter is especially relevant when considering citizens' privacy and data protection, where the citizen may feel a loss of control over their privacy. Likewise, there are other aspects such as identity delegation which are currently included in national legislation, which must be echoed in digital authentication systems and in pan-European legislation.

On the other hand, the initial use of electronic identities in the environment of Public Administration simplifies the problems that can arise and make the solutions feasible in the short term.

The authors of this paper are of the opinion that, despite the issues listed throughout this article, European interoperability will become a reality as these problems are solved and as digital identification systems gain people's trust.

4. Acknowledgements

This paper is part of the work being conducted by the authors in the projects supported by the Ministry of Education and Science of Spain through the National Plan for R+D+I: ADMISSION (TSI2006-4864), Telematic platform for e-Government based on a choreography of services and SEMPERSec (TIN2009-14406-C05-01), Framework for the provision of accessible security guarantees for personal autonomy.

11. References

[1] Various. eGovernment: Commission calls for ambitious objectives in the EU for 2010. [Online] 25 April 2006. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/523&format=PDF&aged=1&language=EN&guiLanguage=en.

[2] The Modinis IDM Study Team. Modinis Study on Identity Management in eGovernment: Common Terminological Framework for Interoperable Electronic Identity Management. Version 2.01. https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc. [Online] 2005. https://www.cosic.esat.kuleuven.be/modinis idm/twiki/bin/view.cgi/Main/GlossaryDoc.

[3] Graux, H. y Majava, J. eID Interoperability for PEGS: Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms. [Online] December 2007. http://ec.europa.eu/idabc/servlets/Doc?id=29622.

[4] A Roadmap for a pan-European eIDM Framework by 2010. Version 1.0. [Online] http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf.

[5] Steel, Christopher, Nagappan, Ramesh y Lai, Ray. Core Security Patterns: Best Practices and Strategies for J2EE™, Web Services, and Identity Management. 1ª. s.l.: Prentice Hall PTR / Sun Microsystems, 2005.

[6] ModinisIDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome.

[7] Bruegger, B. P.; Hühnlein, D. and Schwenk, J.; TLS-Federation - a Secure and Relying-Party-Friendly Approach for Federated Identity Management. http://porvoo14.dvla.gov.uk/documents/tls_federation_final.pdf.

[8] GUIDE, Creating a European Identity Management Architecture for eGovernment, http://istrg.som.surrey.ac.uk/projects/guide/overview.html.

[9] STORK, Secure idenTity acrOss boRders linked, http://www.eid-stork.eu/.

[10] PEPPOL, Pan-European Public Procurement Online. http://www.peppol.eu/.

[11] European Parliament and Council of the European Union. Directive 95/46/CE of the European Parliament and the Council, 24 October 1995, relating to the protection of natural persons as regards the processing of personal data and the free circulation of this data. Official Journal of the European Community. Luxembourg: European Union, 23 November 1995. Vol. L, 281, pgs. 31-50.

[12] Peeters, R.; Simoens, K.; De Cock, D. and Preneel B.; Cross-Context Delegation through Identity Federation, In Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Lecture Notes in Informatics (LNI) P-137, A. Brömme, C. Busch, and D. Hühnlein (eds.), Bonner Köllen Verlag, pp. 79-92, 2008.

[13] Alrodhan, W. and Mitchell, C. J.; A Delegation Framework for Liberty, Proceedings of the 3rd Conference on Advances in Computer Security and Forensics (ACSF'08), Liverpool John Moores University, Liverpool, UK, 10 - 11 July, 2008; pages 67-73.